

# **EXHIBIT A**

**IN THE FIRST JUDICIAL CIRCUIT  
COUNTY OF WILLIAMSON, STATE OF ILLINOIS**

CHARLES HALL, INDIVIDUALLY AND ON BEHALF  
OF ALL OTHERS SIMILARLY SITUATED,

*Plaintiff,*

v.

PEPSI MIDAMERICA CO.,

**Serve:**

**National Registered Agents  
208 S. LaSalle Street, Suite 814  
Chicago, IL 60604**

*Defendant.*

**2018L20**

Case No.:

Judge:

**JURY TRIAL DEMANDED**

**CLASS ACTION COMPLAINT**

Plaintiff Charles Hall (hereinafter "Plaintiff" or "Hall"), brings this Class Action Complaint individually and on behalf of all others similarly situated against Defendant Pepsi MidAmerica Co. ("Defendant" or "Pepsi"), to stop Defendant's unlawful collection, use, storage, and disclosure of Plaintiff's and the proposed Class' sensitive, private, and personal biometric data. Plaintiff alleges as follows upon personal knowledge as to himself and his own acts and experiences and, as to all other matters, upon information and belief including investigation conducted by his attorneys. Further, Plaintiff alleges as follows:

**INTRODUCTION**

1. Plaintiff has worked for Defendant in Illinois, including in Williamson County, Illinois

2. While most employers use conventional methods for tracking time worked (such as ID badge swipes or punch clocks), Defendant mandated and required that its employees have their hands scanned by a biometric timekeeping device.

3. Unlike ID badges or time cards – which can be changed or replaced if stolen or compromised – hand biometrics are unique, permanent biometric identifiers associated with each employee. This exposes Defendant's employees to serious and irreversible privacy risks. For example, if a biometric database is hacked, breached, or otherwise exposed – such as in the recent Equifax data breach – employees have no means by which to prevent identity theft, unauthorized tracking, and other improper or unlawful use of this information.

4. As an employee of Defendant, Plaintiff has been required to “clock in” and “clock out” of work shifts by having his hand scanned by a biometric timeclock which then identified each employee, including Plaintiff.

5. The Illinois Biometric Information Privacy Act (hereinafter “BIPA” or the “Act”) expressly obligates Defendant to obtain an executed, written release from an individual, as a condition of employment, in order to capture, collect, and store an individual's biometric identifiers or biometric information, especially a fingerprint, handprint, or hand geometry scan, and biometric information derived from it.

6. BIPA further obligates Defendant to inform its employees in writing that a biometric identifier or biometric information is being collected or captured; to tell its employees in writing for how long it will store their biometric data or information and any purposes for which biometric information is being captured, collected, and used; and to make available a written policy disclosing when it will permanently destroy such information.

7. BIPA makes all of these requirements a *precondition* to the collection or recording of fingerprints, hand geometry scans, or other associated biometric information – under the Act, no biometric identifiers or biometric information may be captured, collected, purchased, or otherwise obtained if these pre-capture, pre-collection, pre-storage, or pre-obtainment requirements are not met.

8. The State of Illinois takes the privacy of biometric data seriously and its legislature found Illinois citizen's privacy rights warrant strong protections.

9. There is no realistic way, absent surgery, to reassign someone's biometric data. A person can obtain a new social security number, but not a new hand, which makes the protection of, and control over, biometric identifiers and biometric information particularly important – particularly given the increasing use of biometric information or identifiers in the stream of commerce and financial transactions and the ever-increasing rate of corporate data breaches.<sup>1</sup>

---

<sup>1</sup> See, The Council of State Governments E-Newsletter, "Not If, But When" noting "It's not a matter of if a [cybersecurity] breach will happen, but when," said Brenda Decker, Nebraska's chief information officer. The inevitability of a cybersecurity breach—affecting either a private or public institution—was a common sentiment expressed throughout CSG's Cybersecurity and Privacy Policy Academy, held May 6-8 in St. Louis.

There was consensus from private sector representatives like MasterCard, Walmart, Edison Electric Institute and Facebook to state chief information officers and federal officials: both the frequency of cybersecurity threats and their level of sophistication have and will continue to increase.

[http://www.csg.org/pubs/capitolideas/enews/cs17\\_1.aspx](http://www.csg.org/pubs/capitolideas/enews/cs17_1.aspx) (last visited February 5, 2018)

See also, Cyber security: Your Next Breach – Not If, But When? (noting "Gone are the days when businesses can assume that "Cyber attacks won't happen to us". From the recently launched "Ransomware Wanna Cry attack", it has been made crystal clear that cyber attacks are inevitable and can affect not just the banks and credit card companies but any business that has products, services and customers." ). <https://www.collaberatact.com/cyber-security-next-breach-not/> (last visited February 5, 2018).

10. While Defendant may claim that a data breach is unlikely to occur, that narrow view does not comport with the overwhelming view of data security experts, which can be best summarized by the phrase, "it's not if, but when."

11. Defendant captured, collected, received through trade, and/or otherwise obtained and biometric identifiers or biometric information of their Illinois employees, like Plaintiff, without properly obtaining the above-described written executed release, and without making the required disclosures concerning the collection, storage, use, or destruction of biometric identifiers or information.

12. Additionally, upon information and belief, Plaintiff and the Class members are aggrieved because Defendant improperly discloses employees' biometric data to out-of-state third-party vendors in violation of BIPA.

13. Upon information and belief, Defendants lack retention schedules and guidelines for permanently destroying Plaintiff's and the Class' biometric data and has not and will not destroy Plaintiff's or the Class' biometric data as required by BIPA.

14. Plaintiff and the putative Class are aggrieved by Defendant's failure to destroy their biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of employees' last interactions with the company.

15. Plaintiff and the putative Class have suffered an injury in fact based on Defendant's violations of their legal rights.

16. Plaintiff seeks damages and injunctive relief for Defendant's BIPA violations, for himself and all those similarly situated.

#### **PARTIES, JURISDICTION, AND VENUE**

17. Plaintiff Charles Hall is an individual citizen of the State of Illinois.

18. Defendant Pepsi MidAmerica Co. is an Missouri corporation that is registered with the Illinois Secretary of State to do business in Illinois. Pepsi MidAmerica Co. is located at 2605 West Main, Marion, Illinois.

19. Defendant Pepsi MidAmerica Co. may be served through its registered agent, 208 South LaSalle Street, Suite 814, Chicago, Illinois 60604.

20. Jurisdiction is proper in this Court as Plaintiff is a citizen of Illinois and Defendant is organized under the laws of the State of Illinois.

21. Venue is proper in this court pursuant to 735 ILCS 5/2-101 as a substantial part of the transactions at issue took place in Cook County, namely, at Defendant's location in Williamson County.

#### **PLAINTIFF SPECIFIC ALLEGATIONS**

22. Plaintiff was, during relevant times, employed by Defendant.

23. Plaintiff was required to "clock-in" and "clock-out" using a timeclock that operated, at least in part, by scanning Plaintiff's hand geometry.

24. As a new employee, Plaintiff was required to scan his hand multiple times so Defendant could create, collect, capture, construct, store, use, and/or obtain a biometric template for Plaintiff.

25. Defendant then used Plaintiff's biometrics as an authentication method to track his time, potentially with the help of a third-party vendor.

26. Defendant subsequently stored Plaintiff's biometrics data in its database(s).

27. Each time Plaintiff began and ended his workday, he was required to scan his hand.

28. Plaintiff has never been informed of the specific limited purposes or length of time for which Defendant collected, stored, or used his biometrics.

29. Plaintiff has never been informed of any biometric data retention policy developed by Defendant, nor has he ever been informed of whether Defendant will ever permanently delete his biometrics.

30. Plaintiff has never been provided with nor ever signed a written release allowing Defendant to collect, capture, store, or otherwise obtain his hand print, hand geometry, or other biometrics.

31. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by Defendant's violations of BIPA alleged herein.

32. A showing of actual damages is not necessary in order to state a claim under BIPA.

33. Nonetheless, Plaintiff and the putative Class suffered actual, concrete injuries in fact based on Defendant's violations of Plaintiff's legal rights.

34. Additionally, Plaintiff suffered an invasion of a legally protected interest when Defendant secured his personal and private biometric data at a time when it had no right to do so, an invasion of Plaintiff's and the putative Class' right to privacy.

35. BIPA protects employees like Plaintiff and the putative Class from this precise conduct, and Defendant had no right to secure this data absent a specific legislative license to do so.

36. Plaintiff and the putative Class also suffered an informational injury because no Defendant provided them with information to which they were entitled by statute.

37. Through BIPA, the Illinois legislature has created a right – an employee's right to receive certain information prior to an employer securing their highly personal, private and proprietary biometric data – and an injury – not receiving this extremely critical information.

38. Pursuant to 740 ILCS 14/15(b), Plaintiff and the putative Class were entitled to receive certain information prior to Defendant securing their biometric data; namely, information advising them of the specific limited purpose(s) and length of time for which it collects, stores, and uses their hand biometrics; information regarding Defendants' biometric retention policy; and, a written release allowing Defendants to collect and store their private biometric data.

39. By depriving Plaintiff of this information, Defendants injured him and the putative Class he seeks to represent. *Public Citizen v. U.S. Department of Justice*, 491 U.S. 440, 449 (1989); *Federal Election Commission v. Akins*, 524 U.S. 11 (1998).

40. Finally, as a result of Defendant's conduct, Plaintiff has experienced personal injury in the form of mental anguish.

41. For example, Plaintiff experiences mental anguish, emotional distress, and injury when contemplating what would happen to his biometric data if Defendant ever choose to sell, lease, license, publish, or release his biometrics, or what would happen if Defendant went bankrupt, was sold, franchised, acquired, or merged with another entity, whether Defendant will ever delete his biometric information, and whether (and to whom) Defendant currently or may in the future share his biometric information with.

#### **ILLINOIS'S STRONG STANCE ON PROTECTION OF BIOMETRIC INFORMATION**

42. In the early 2000s, major national corporations started using Chicago and other locations in Illinois to test "new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS 14/5(c). Given its relative infancy, an overwhelming portion of the public became weary of this then-growing yet unregulated technology. See 740 ILCS 14/5.



43. In late 2007, a biometrics company called Pay by Touch, which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions, filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records – which, like other unique biometric identifiers, can be linked to people’s sensitive financial and personal data – could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who had used that company’s fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

44. Recognizing the “very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information,” Illinois enacted BIPA in 2008. See Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS 14/5.

45. Additionally, to ensure compliance, BIPA provides that, for each violation, the prevailing party may recover \$1,000 or actual damages, whichever is greater, for negligent violations and \$5,000, or actual damages, whichever is greater, for intentional or reckless violations. 740 ILCS 14/20.

46. BIPA provides valuable privacy rights, protections, and benefits to employees in Illinois.

47. For example, BIPA’s requirements ensure that the environment for taking of biometrics is not forced or coerced; that individuals are freely advised that, by scanning one’s hand, the employer is capturing, extracting, creating, and recording hand biometrics; that

individuals can keep tabs on their biometric roadmaps (*e.g.*, who has their biometrics, for long how, and how it is being used), including after one's employment ceases, or after the employer stops storing the employee's biometrics if at all, when employer-employee files or policies may not be freely accessible; that individuals can evaluate the potential consequences of providing their biometrics; that companies must give individuals the right, and opportunity, to freely consent (or decline consent) before taking their biometrics; that, if the disclosure does not say so, the employee's biometrics will not be used for any other purpose except for employee time and attendance and will not be used to run a criminal background check; and that their biometrics are being handled with a measure of security. The BIPA-required environment for the taking of biometrics provides legislatively-imposed peace for biometric subjects.

48. To this end, in passing the Biometric Information Privacy Act (hereinafter "the Act"), the Illinois General Assembly found:

- (a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.
- (b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.
- (c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.
- (d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.

- (e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.
- (f) The full ramifications of biometric technology are not fully known.
- (g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

See, 740 ILCS 14/5, Legislative findings; intent.

49. The law is specifically designed to require a company that collects biometrics to jump through several hoops, *before collection*, aimed, in part, at educating and protecting the person whose biometrics it is taking for its own use, and requiring signed, written consent attesting that the individual has been properly informed and has freely consented to biometrics collection.

50. The Act defines "Biometric identifier" as:

a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

See, 740 ILCS 14/10.

51. The Act defines "Biometric information" as:

any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric

information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

See, 740 ILCS 14/10.

52. The Act defines "Confidential and sensitive information" as:

personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.

See, 740 ILCS 14/10.

53. The Act defines "Private entity" as:

any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.

See, 740 ILCS 14/10.

54. The Act defines "Written release" as:

informed written consent or, in the context of employment, a release executed by an employee as a condition of employment

See, 740 ILCS 14/10.

55. The Act requires:

A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

740 ILCS 14/15(a).

56. Additionally, the Act provides:

No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

740 ILCS 14/15(b).

57. Further, the Act provides:

No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

740 ILCS 14/15(c).

58. The Act also provides:

No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

740 ILCS 14/15(d).

59. Furthermore, the Act provides:

A private entity in possession of a biometric identifier or biometric information shall:

(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

740 ILCS 14/15(e).

60. BIPA provides statutory damages if an employer takes an employee's biometrics and invades an employee's privacy by circumventing BIPA's preconditions and requirements.

61. The Act explicitly provides a private right of action for violations of the Act, and provides that a prevailing party "may recover for each violation:"

(1) against a private entity that negligently violates a provision of this Act, liquidated damages of \$1,000 or actual damages, whichever is greater;

(2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of \$5,000 or actual damages, whichever is greater;

(3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

(4) other relief, including an injunction, as the State or federal court may deem appropriate.

740 ILCS 14/20.

62. In enacting BIPA, the Illinois General Assembly explicitly singled out and bound employers to BIPA's requirements. 740 ILCS § 14/10 (defining "Written release" in the context of employment); 740 ILCS § 14/15(b)(3).

63. Therefore, employees whose rights under BIPA are violated clearly fall within BIPA's zone-of-interest of protection.

64. In fact, BIPA requires express written consent not only in order to capture or collect biometrics in the first place, but in the context of employment, the requirement goes a step further: the employer must obtain "informed written consent," in the form of "a release executed by an employee," and further, the release must be executed "as a condition of employment." *Id.* These formalized protections enable employees to freely consent to the taking of their biometrics.

65. Defendant violated these clear protections of the Act; Defendant violated, and upon information and belief, continues to violate its employees' biometric, privacy, informational, and statutory rights.

#### **DEFENDANT'S BIOMETRIC HAND-SCANNING OF EMPLOYEES**

66. By the time BIPA passed through the Illinois Legislature in mid-2008, most employers who had experimented using consumers' biometric data stopped doing so or did so in compliance with the law.

67. Unfortunately, Defendant failed to take note of the shift in Illinois law governing the collection and use of biometric data. As a result, Defendant continues to collect, store, and use Plaintiff's and the Class' biometric data in violation of BIPA.

68. At relevant times, Defendant has taken the rather invasive and coercive step of requiring employees to be hand scanned, and then using biometric information captured from those hand scans, and data derived therefrom, to identify the employee and track employee work time.

69. After an employee's hand scan is captured, collected, and/or recorded by Defendant, employees are subsequently required to scan their hand into one of Defendant's biometric time clocks when they clock in or out at work.

70. Defendant captures, collects, stores, and/or otherwise obtains the employee's biometrics in order to identify and verify the authenticity of the employee who is clocking in or out.

71. Moreover, Defendant causes these biometrics to be associated with employees, along with other employee personal and work information.

72. Defendant has a practice of using biometric time clocks to track its employees, albeit without regard to Illinois' requirements under BIPA.

73. As part of the employee time-clocking process, Defendant caused biometrics from employee hand scans to be recorded, collected, captured, and stored at relevant times.



74. Defendant did not give Plaintiff or Class members any choice in the use of biometric timeclocks.

75. Defendant has not, on information and belief, properly informed its employees in writing that a biometric identifier or biometric information is being captured, obtained, collected or stored; informed its employees in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; obtained employees' proper written consent to the capture, collection, obtainment or storage of their biometric identifier and biometric information derived from it; or obtained employees' executed written release as a condition of employment.

76. Defendant employed Plaintiff in Williamson County, Illinois.

77. At relevant times, in Williamson County, Illinois, Defendant instituted and enforced a biometric time clock scheme whereby they initially took Plaintiff's hand scan, and subsequently required Plaintiff to scan his hand when clocking in and out of work, pursuant to which Defendant collected, captured, stored, and/or otherwise obtained Plaintiff's hand geometry scan and biometrics derived from it.

78. Use of the biometric timekeeping system was not made a condition of employment.

79. When Plaintiff arrived for work, and when Plaintiff left or clocked in or out of work, at relevant times during his employment, Defendant required Plaintiff to submit Plaintiff's hand geometry scan to Defendant's timekeeping system. The system captured, collected, stored, and/or otherwise obtained Plaintiff's biometrics.

80. Defendant further required Plaintiff to scan Plaintiff's hand in order to use the biometric system, so that the timekeeping system captured, collected, stored, and/or otherwise obtained Plaintiff's hand scan, matched Plaintiff's hand scan biometrics, and associated Plaintiff's biometrics with Plaintiff's identity.



81. Defendant did not at any time, on information and belief, inform Plaintiff in writing (or otherwise) that a biometric identifier and biometric information was being obtained, captured, collected, and/or stored, or of the specific purposes and length of term for which a biometric identifier or biometric information was being collected, captured, stored, and/or used; obtain, or attempt to obtain, Plaintiff's executed written release to have Plaintiff's biometrics captured, collected, stored, or recorded as a condition of employment – Plaintiff did not provide consent required by BIPA to the capture, collection, storage, obtainment, and/or use Plaintiff's hand or associated biometrics. Nor did Plaintiff know or fully understand that Defendant was collecting, capturing, and/or storing biometrics when Plaintiff was scanning Plaintiff's hand; nor did Plaintiff know or could Plaintiff know all of the uses or purposes for which Plaintiff's biometrics were taken.

82. Through these acts, Defendant has not only violated the BIPA, but has also violated Plaintiff's right to privacy.

83. Defendant has not publicly disclosed its retention schedule and guidelines for permanently destroying employee biometrics, if they exist.

84. Defendant, on information and belief, has no written policy, made available to the public, that discloses its retention schedule and or guidelines for retaining and then permanently destroying biometric identifiers and information.

85. The Pay by Touch bankruptcy that catalyzed the passage of BIPA highlights why conduct such as Defendants' – where individuals are aware that they are providing a biometric but not aware of to whom or for what purposes they are doing so – is dangerous.

86. That bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers or information such as a fingerprint, and/or data derived therefrom, who exactly is collecting their biometric data, where it will be transmitted and for what purposes, and for how long.

87. Thus, BIPA is the Illinois Legislatures expression that Illinois citizens have biometric privacy rights, as created by BIPA.

88. Defendant disregards these obligations and instead unlawfully collects, stores, and uses employees' biometric identifiers and information, without ever receiving the individual's informed written consent as required by BIPA.

89. Defendant's employees are not told what might happen to their biometric data if and/or when their local stores are sold, taken over by different management, re-franchises, or, worse, if and when Defendant's entire enterprise folds.

90. Because Defendant neither publishes a BIPA-mandated data retention policy nor disclose the purposes for their collection of biometric data, Defendant's employees have no idea whether Defendant sells, discloses, re-discloses, or otherwise disseminates his or her biometric data.

91. Nor are Plaintiff and the putative Class told whom Defendant currently discloses his or her biometric data, or what might happen to his or her biometric data in the event of a buyout, merger, or a bankruptcy.

92. These violations have raised a material risk that Plaintiff and the putative Class' biometric data will be unlawfully accessed by third parties.

93. By and through the actions detailed above, Defendant does not only disregard the Class' privacy rights, but they also violate BIPA.

94. Defendant's above-described use of biometrics benefits only Defendant. There is no corresponding benefit to employees: Defendant has required, or coerced, employees to comply in order to receive a paycheck, after they have been committed to the job.

### CLASS ALLEGATIONS

95. Plaintiff brings this action on behalf of himself and pursuant to 735 ILCS 5/2-

801 on behalf of a class (hereinafter the "Class") defined as follows:

All persons who were enrolled in the biometric timekeeping system and subsequently used a biometric timeclock at Pepsi MidAmerica Co. from five years preceding the filing of this action to the date a class notice is mailed in this action.

Excluded from the class are Defendant's officers and directors, Plaintiff's counsel, and any member of the judiciary presiding over this action.

96. **Numerosity:** The exact number of class members is unknown and is not available to Plaintiff at this time, but upon information and belief, there are in excess of forty potential class members, and individual joinder in this case is impracticable. Class members can easily be identified through Defendant's records and allowing this matter to proceed on a class basis will prevent any retaliation by Defendant against current employees who are currently having their BIPA rights violated.

97. **Common Questions:** There are several questions of law and fact common to the claims of Plaintiff and the Class members, and those questions predominate over any questions that may affect individual Class members. Common questions include, but are not limited to, the following:

- a. whether Defendant has a practice of capturing or collecting employees' biometrics;
- b. whether Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of the individual's last interaction with Defendant, whichever occurs first;
- c. whether Defendant obtained an executed written release from hand scanned employees before capturing, collecting, or otherwise obtaining employee biometrics;
- d. whether Defendant obtained an executed written release from hand scanned

employees, as a condition of employment, before capturing, collecting, converting, sharing, storing or using employee biometrics;

- e. whether Defendant provided a writing disclosing to employees the specific purposes for which the biometrics are being collected, stored, and used;
- f. whether Defendant provided a writing disclosing to hand scanned employees the length of time for which the biometrics are being collected, stored, and used;
- g. whether Defendant disclosed or re-disclosed biometric identifiers or biometric information to third parties;
- h. whether Defendant's conduct violates BIPA;
- i. whether Defendant's violations of BIPA have raised a material risk that Plaintiff's and the putative Class' biometric data will be unlawfully accessed by third parties
- j. whether Defendant's conduct was negligent, reckless, or willful;
- k. whether Plaintiff and Class members are entitled to damages, and what is the proper measure of damages;
- l. whether Plaintiff and Class members are entitled to injunctive relief.

98. **Adequacy of Representation:** Plaintiff will fairly and adequately represent and protect the interest of the class, and has retained competent counsel experienced in complex litigation and class action litigation. Plaintiff has no interests antagonistic to those of the class, and Defendant has no defenses unique to Plaintiff.

99. **Appropriateness:** Class proceedings are also superior to all other available methods for the fair and efficient adjudication of this controversy because joinder of all parties is impracticable. Further, it would be virtually impossible for the individual members of the Class to obtain effective relief because of the fear and likelihood of retaliation by Defendant against current employees bringing a civil action as an individual. Even if Class members were able or willing to pursue such individual litigation, a class action would still be preferable due to the fact that a multiplicity of individual actions would likely increase the expense and time of litigation given the

complex legal and factual controversies presented in this Class Action Complaint. A class action, on the other hand, provides the benefits of fewer management difficulties, single adjudication, economy of scale, and comprehensive supervision before a single Court, and would result in reduced time, effort and expense for all parties and the Court, and ultimately, the uniformity of decisions.

**COUNT I – FOR DAMAGES**  
**VIOLATION OF 740 ILCS 14/1, ET SEQ. – THE BIOMETRIC INFORMATION PRIVACY ACT**  
**INDIVIDUALLY AND ON BEHALF OF THE CLASS**

100. Plaintiff, individually and on behalf of all others similarly situated, repeats, re-alleges, and incorporates all preceding paragraphs as if fully set forth herein.

101. BIPA is a remedial statute designed to protect employees, by requiring consent and disclosures associated with the handling of biometrics, particularly in the context of biometric technology. 740 ILCS 14/5(g), 14/10, and 14/15(b)(3).

102. The Illinois General Assembly's recognition of the importance of the public policy and benefits underpinning BIPA's enactment, and the regulation of biometrics collection, is detailed in the text of the statute itself.

103. Defendant has been and continues to be a "private entity."

104. Defendant has been and continues to be a "private entity" in possession of Plaintiff's and other employees' biometrics, and it collected, captured, or otherwise obtained their biometric identifiers and biometric information within the meaning of the Act.

105. As more fully set forth above, at relevant times Defendant collected, captured, or otherwise obtained, Plaintiff's and other employees' biometric identifiers and biometric information based on those identifiers as defined by BIPA, 740 ILCS 14/10, through the imposition of biometric hand geometry scanning time clocks.

106. In violation of 740 ILCS 14/15(a), Defendant failed to make such a written policy publicly available to Plaintiff and other class members.

107. In violation of 740 ILCS 14/15(b), Defendant has collected, captured, stored, and/or otherwise obtained Plaintiff's and other class members' biometric identifiers and biometric information, without:

- a. informing Plaintiff and the Class (including, where applicable, their legal authorized representatives), in writing, that the biometric identifiers or biometric information were being obtained, collected, captured, and/or stored;
- b. informing Plaintiff and the Class (including, where applicable, their legal authorized representatives), in writing, of the specific purpose and length of term for which the biometric identifiers or biometric information were being collected, stored, and used; and
- c. receiving a written release executed by Plaintiff and/or Class members, and executed by Plaintiff and/or Class members as a condition of employment.

108. Defendant took Plaintiff's and other class members' hand scans, and knowingly caused their biometrics to be captured, collected, stored, and/or otherwise obtained without making publicly available the required policy that explains, for example, any purposes for which the biometric identifiers and information were collected, a retention schedule, and guidelines for permanently destroying biometric identifiers and information.

109. BIPA also prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

110. As a result of Defendant's above-described acts and omissions, Defendant has invaded the statutory biometric rights and the privacy rights of Plaintiff and the Class; it has unlawfully and coercively taken their biometrics; it has failed to provide them with information required by BIPA; it has deprived them of benefits, rights, opportunities and decisions conferred and required by the Illinois legislature via BIPA; it has caused harm, including mental anguish and

emotional distress, and it illegally captured, collected, recorded, possessed, converted, and/or stored their hand scans, biometrics, and property.

111. Upon information and belief, Defendant systematically disclosed Plaintiff's and the Class's biometric identifiers and biometric information to out-of-state third-party vendors.

112. Accordingly, Defendant has violated BIPA, and Plaintiff and the Class have been damaged and are entitled to damages available under the BIPA, including liquidated damages of \$1,000 per violation, or actual damages, whichever is greater. 740 ILCS 14/20(1).

#### **PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff, individually and on behalf of the Class of similarly situated individuals, prays for an Order as follows:

- A. Finding this action satisfies the prerequisites for maintenance as a class action set forth in 735 ILCS 5/2-801, *et seq.*, and certifying the Class as defined herein;
- B. Designating and appointing Plaintiff as representative of the Class and Plaintiff's undersigned counsel as Class Counsel;
- C. Entering judgment in favor of Plaintiff and the Class and against Defendant;
- D. Awarding Plaintiff and the Class members liquidated damages of \$5,000 *per each violation* found to be willful and/or reckless, \$1,000 *per each violation* found to be negligent, or actual damages, at the election of Plaintiff, or whichever is greater, for each violation of BIPA;
- E. Awarding Plaintiff and the Class members reasonable attorneys' fees and costs incurred in this litigation; and
- F. Granting all such other and further relief as the Court deems just and appropriate.



**COUNT II – FOR INJUNCTIVE RELIEF**  
**VIOLATION OF 740 ILCS 14/1, ET SEQ. – THE BIOMETRIC INFORMATION PRIVACY ACT**

113. Plaintiff, individually and on behalf of all others similarly situated, repeats, re-alleges, and incorporates all preceding paragraphs as if fully set forth herein.

114. BIPA provides for injunctive relief. 740 ILCS 14/20(4).

115. Plaintiff and other Class members are entitled to an order requiring Defendant to make disclosures consistent with the Act and enjoining further unlawful conduct.

116. First, Plaintiff seeks an order requiring Defendant to publicly disclose a written policy establishing any specific purpose and length of term for which Plaintiff and other employees' biometrics have been collected, captured, stored, obtained, and/or used, as well as guidelines for permanently destroying such biometrics when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first, as required by 740 ILCS 14/15(a).

117. Second, Plaintiff seeks an order requiring Defendant to disclose whether Defendant has retained Plaintiff's and other employees' biometrics in any fashion, and if, when, and how such biometrics were permanently destroyed, consistent with BIPA.

118. Third, due to the above-described facts, and Defendant's failure to make publicly available facts demonstrating BIPA compliance as BIPA requires, Defendant should be ordered to: (i) disclose if (and if, precisely how, and to whom) it has disseminated, sold, leased, traded, or otherwise profited from Plaintiff and other hand scanned employees' biometrics, which is strictly prohibited under BIPA; and (ii) disclose the standard of care that it employed to store, transmit, and protect such biometrics, as provided under BIPA. 740 ILCS 14/15(c), (d), (e).

119. Fourth, Defendant should be enjoined from further BIPA non-compliance, and should be ordered to remedy any BIPA compliance deficiencies forthwith.



120. Plaintiff's and other Class members' legal interests are adverse to Defendant's legal interests. There is a substantial controversy between Plaintiff and Class members and Defendant warranting equitable relief so that Plaintiff and the Class may obtain the protections that BIPA entitles them to receive.

121. Plaintiff and the Class do not know what Defendant has done (or intends to do) with their biometrics. Absent injunctive relief, Defendant is likely to continue its BIPA non-compliance and Plaintiff and other Class members will continue to be in the dark on the subject.

122. For the reasons set forth above, Plaintiff is likely to succeed on the merits of Plaintiff's claims.

123. BIPA establishes the importance, value, and sensitive nature of biometrics, along with the need to protect and control it; Plaintiff is entitled to know what Defendant has done with it as set forth above, and to an affirmation and verification that it has been or will be permanently destroyed as required by 740 ILCS 14/15(a).

124. The gravity of the harm to Plaintiff and the Class, absent equitable relief, outweighs any harm to Defendant if such relief is granted.

125. As a result, Plaintiff requests commensurate injunctive relief.

**WHEREFORE**, Plaintiff, individually and on behalf of the class, prays for an Order as follows:

- A. Finding this action satisfies the prerequisites for maintenance as a class action set forth in 735 ILCS 5/2-801, *et seq.*, and certifying the class defined herein;
- B. Designating and appointing Plaintiff as representative of the class and Plaintiff's undersigned counsel as class counsel;
- C. Entering judgment in favor of Plaintiff and the class and against Defendant;

- D. Awarding Plaintiff and the class members all damages available to Plaintiff and the class available under applicable law, including statutory or liquidated damages;
- E. Providing commensurate injunctive relief for Plaintiff and class members as set forth above;
- F. Awarding Plaintiff and the Class members reasonable attorneys' fees and costs incurred in this litigation; and
- G. Granting all such other and further relief as the Court deems just and appropriate.

**JURY DEMAND**

Plaintiff demands a trial by jury on all issues so triable.

Respectfully submitted,

Dated: February 5, 2017

By: /s/ Brandon M. Wise  
Brandon M. Wise – IL Bar # 6319580  
Paul A. Lesko – IL Bar # 6288806  
PEIFFER ROSCA WOLF  
ABDULLAH CARR & KANE, APLC  
818 Lafayette Ave., Floor 2  
St. Louis, MO 63104  
Ph: 314-833-4825  
Email: [bwise@prwlegal.com](mailto:bwise@prwlegal.com)  
Email: [plesko@gmail.com](mailto:plesko@gmail.com)

COUNSEL FOR THE PLAINTIFF AND THE  
PUTATIVE CLASS

IN THE FIRST JUDICIAL CIRCUIT  
COUNTY OF WILLIAMSON, STATE OF ILLINOISCHARLES HALL, INDIVIDUALLY AND ON BEHALF  
OF ALL OTHERS SIMILARLY SITUATED,*Plaintiff,*

v.

PEPSI MIDAMERICA CO.,

Serve:

National Registered Agents  
208 SO LaSalle Street, Suite 814  
Chicago, IL 60604*Defendant.*

2018L20

Case No.:

Judge:

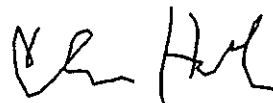
JURY TRIAL DEMANDED

## AFFIDAVIT

I, Charles Hall, declare as follows:

1. My name is Charles Hall and I reside in Williamson County, Illinois.
2. I have reviewed the Class Action Complaint to be filed in this matter, and believe it to be true and to the best of my knowledge.
3. I believe that Pepsi MidAmerica Co. harmed me and other people who worked for Pepsi MidAmerica Co. by violating the Illinois Biometric Information Privacy Act.
4. I believe that I and all other similarly situated people are entitled to damages in excess of \$50,000 for the damages caused by Pepsi MidAmerica Co.

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the statements set forth in this instrument are true and correct, except as to matters therein stated to be on information and belief and as to such matters the undersigned certifies as aforesaid that he verily believes the same to be true.



Charles Hall